IT GOVERNANCE NETWORK

Impact of the POPI Act on Cloud Computing

Complying with the Protection of Personal Information Act

The Protection of Personal Information Act stipulates that every public and private body is responsible for the processing of personal information in their possession or under their control. When a Cloud Provider is engaged by a customer (responsible party) to process personal information, a written contract with the responsible party is required to clarify responsibility for potential legal consequences, record knowledge of the services being provided and establish control.

Cloud Providers engaged to provide services

Cloud providers domiciled in the Republic; or if not domiciled in the Republic, but making use of automated means in the Republic, must comply with all the conditions for the lawful processing of personal information as set forth in the Protection of Personal Information Act.

Cloud providers must, as a minimum, implement and maintain appropriate technical and organizational measures to keep personal information secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage.

When a cloud provider does not have a contract with a responsible party, or if the contract is suspended or terminated, the cloud provider is responsible for the personal information in its possession, or under its control and may be prosecuted for the unlawfully processing of personal data.

Liability of Cloud Providers

Cloud providers (being operators) are not liable for using personal data illegally unless they breach the contract with the organisation (responsible party) for whom they are authorised to process personal information. However, cloud providers are liable for all other personal data in their possession or under their control.

Contracts between responsible parties and the cloud providers serve to clarify who is accountable for the services being provided, the personal data in the possession of the cloud providers and the processing instructions that were given by the responsible parties to the cloud providers.

Cloud providers in possession or control of personal data are the responsible party for all personal information not being processed in accordance with a written contract and are liable for any unlawful processing not covered by a contract.

Cloud Provider: Responsible Party or Operator

The fact that a cloud provider provides a service to another organisation does not necessarily mean that the cloud provider is acting as an operator. It could be that the cloud provider is a responsible party in its own right, depending on the degree of control it exercises over the processing operation.

A cloud provider processing personal data of data subjects must enable data subjects to exercise their rights and in particular, enable a data subject to determine, free of charge, whether or not the responsible party holds any of his, her or its personal information. The cloud provider is required to provide the information within a reasonable time, manner and format.

Cloud Providers need permission

In the event that a cloud provider needs to access personal information to execute an instruction or provide technical support, the cloud provider must have first received permission for such access from the responsible party or, alternatively, directly from the data subject. Moreover, the Cloud Provider must know the name of the contact person who can grant the required access rights.

A cloud provider may only use personnel who are subject to a binding obligation to observe confidentiality when fulfilling their contractual obligations and because of the risk of non-compliance with the statutory obligation to process personal information lawfully, the cloud provider must ensure that all staff who access and process personal information are properly trained.

Protecting Personal Information

Cloud providers must implement and maintain the measures necessary to comply with the conditions for the lawful processing of personal information.

A cloud provider's protection measures are inadequate if the cloud client (data subject) does not have control over the organisational and technical measures that the cloud service provider has deployed.

Data subjects have the right to lodge a claim or to raise a dispute to achieve a remedy. The Information Regulator may also intervene by requesting or enforcing the blocking, erasure or destruction of data or even shutting off the operator's system.

It is essential that the responsible party be able to effectively control the cloud provider and to use the IT systems to influence or stop the data processing at any time.

Service provider Verification

Regardless of the nature of the services or the location of the infrastructure, cloud providers are required to be fully transparent about their processing of personal information.

Data subjects are entitled to know the precise physical location of their personal information, the specific devices where the personal data physically exists, including temporary storage, who has accessed their data, for what purpose and what safeguards are in place to protect the data subjects rights.

Consequently responsible parties are required at least annually to verify that the technical and organisational measures implemented and maintained by a cloud provider are effective in safeguarding their data subjects' rights.

Responsible parties may not use cloud providers that are unable to process personal information lawfully.

 www.itgovernance.co.za cell: 0825588732 info@itgovernance.co.za